



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/576,412

05/22/2000

Gilles Lisimaque

032326-025

1838

21839

7590

01/27/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER

DADA, BEEMNET W

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/576,412

Applicant(s)

LISIMAQUE, GILLES

Examiner

Beemnet W Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in reply to an amendment filed on September 16, 2004. New claims 14-17 have been added. Claims 1-17 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-8 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over leki et al (hereinafter leki), US Patent 5,204,512, in view of Chen et al (hereinafter Chen), US Patent 5,694,471, and further in view of Bosen et al, US Patent 5,060,263.

4. As per claims 1 and 14, leki discloses a means of managing data stored in a first memory of a first chip card of a first chip card (see abstract) in which:

a first management code is recorded in the first memory (see for example; col 3 In 58-col 4 In 4), the first card is linked to a chip card reader (see for example; card detectors, col 3 In 25-31 and fig 1), and editing of data stored in the first memory is authorized if a secret code (code number or password) presented to the reader is compatible with the recorded first management code (see for example; col 3 In 64-col 4 In 4), wherein the following steps are performed:

data relating to the first card and the second management code are recorded in a second memory of a second chip of the second chip card (see for example; col 4 ln 38-46 and col 4 ln 62-67), and editing of the data stored in the second memory is authorized if a secret code (code number or password) presented to the reader is compatible with the recorded second management code (see for example; col 4 ln 32-46).

leki does not explicitly teach a first management code produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card. Chen further discloses a method of access protection on a chip card including producing a management code (PIN) with a first cryptographic algorithm (encryption) and a set of identification data of the first chip card (see for example; col 8 ln 46-59). Chen further discloses the means of such generation of management codes provide a means of higher security and authenticity of the cards (see for example; col 3 ln 26-41). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use the management code generation of Chen within the system of leki to generate the management code because it would have provided a secure means of generating a management code that is high in authenticity in the system of leki. leki-Chen discloses the means of generating a management codes for a chip card based on identification data of the chip card and authorizing editing of data stored in the memory of the chip card, as described above. leki-Chen does not explicitly teach generation of a second management code with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card. Bosen discloses a access control system comprising of dynamic management codes (see for example; col 4 ln 1549) wherein the second management code is generated based on prior data and new data (see for example; col 4 ln 27-49 col 6 ln 58-67) and that such generation can be carried out by a chip card (see for example; portable password issuing devices, col 4 ln 50-62). Bosen

further discloses use of dynamic passwords being well known in the art to promote security since passwords are generated dynamically and are linked to each other (see for example; col 4 In 2749). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bosen within the leki-Chen combination because it would have provided a means of generating a second management code, which is linked with a first management code. In smart card replacements, linking of the second card with a first card is well known in the art and further provides an extra layer of authenticity of the replacement card.

5. As per claims 2, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). leki further discloses the first and second management codes are secret codes (see for example; col 3 In 64-67 and col 4 In 38-46; Such use of code number implies that the first and second management codes must be secret codes to keep the integrity and purpose of the codes for authorization requests).

6. As per claim 3, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Chen further discloses that the cryptographic algorithms are performed in the chip of the card (see for example; col 8 In 46-59) and is rejected under the same rationale of producing management codes described above (see claim 1).

7. As per claim 4, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). leki discloses a first cryptographic algorithm for communication being different from a second cryptographic algorithm (see for example; col 2 In 12-24). Switching cryptographic algorithms are well known in the art to increase security by eliminating attacks by

Art Unit: 2135

trial and error and reverse engineering. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate such switching of algorithms because it would have provided an increase in code integrity by avoiding such attacks. Bosen further discloses the second cryptographic algorithm is symmetric (see for example; DES, col 4 ln 63-65). Such algorithms are rejected under the same rationale of dynamic passwords as described above (see claim 1).

8. As per claims 5 and 15, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Bosen further discloses that the first cryptographic algorithm is the same as the second cryptographic algorithm (see for example; DES, col 4 ln 63-65). Such algorithms are rejected under the same rationale of dynamic passwords as described above (see claim 1).

9. As per claims 6 and 16, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Chen further discloses generating management codes using data relating to a first card and that the use of such a generating means increases protection of forgery and duplication of an existing card by copying. One of ordinary skill in the art at the time of the applicant's invention would have realized that in such a combination, generation of passwords are based on identification. It would have been obvious for such generation of passwords in the leki-Chen-Bosen combination because it would have provided additional protection of card fraud and copying.

10. As per claim 7, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). As per the data relating to the first card is the first management code of the first card or the first chip card, Bosen further discloses the prior data being a first management code

(see for example; col 4 ln 27-32). Such data for generating a second management code is rejected under the same rationale of management code generating described above (see claim 1).

11. As per claim 8, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). leki does not explicitly teach a determination of whether the card is authentic. Chen further discloses a determination being made of whether the card is authentic if said management code word produced in the reader on the basis of the data relating to the first card is compatible with a second key word (see for example; digital signature, col 9 ln 56-col 10 ln 11), and that such determination of authenticity prevents cards from being duplicated by copying (see for example; col 3 ln 26-41). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the determination means of Chen within the system of leki because it would have increased security and authenticity by preventing card forgery and copying.

12. Claims 9-13, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over leki et al (hereinafter leki), US Patent 5,204,512, in view of Chen et al (hereinafter Chen), US Patent 5,694,471, and further in view of Bosen et al, US Patent 5,060,263, and further in view of Drupsteen et al, US Patent 6,073,236.

13. As per claims 9 and 17, leki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). leki-Chen-Bosen does not disclose a transmission attribute associated with the data stored in the first memory. Drupsteen discloses storing the data with a transmission attribute (flag register, col 4 ln 17-39), the use of attributes to specify commands to be

processed (col 5 ln 17-39), and copying of the attribute into a memory (flag register associated with master file, fig 4, col 5 ln 17-39). As for the attribute giving information about a need to produce a second secret code when copying data, Drupsteen further discloses the use of attributes to specify commands to be processed (col 5 ln 17-39). One of ordinary skill in the art at the time of the applicant's invention would have modified the leki-Chen-Bosen combination to further associate a transmission attribute with data stored in the first memory. Both the leki-Chen-Bosen combination and Drupsteen discloses a method of managing data in a chip card and transmission of data from a card. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the leki-Chen-Bosen combination because it would have added flexibility to the chip card. The addition of attributes can allow the chip card to perform certain commands depending on the attribute.

14. As per claim 10, leki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). leki further discloses editing of data under the control of a master system (see for example; col 4 ln 47-63). leki-Chen-Bosen does not explicitly teach reading an attribute prior to editing and an editing program is started if the attribute having been read allows this. Drupsteen discloses reading the attributes before processing a command (col 5 ln 17-28) and use of attributes to inhibit or allow certain commands to be processed (col 5 ln 17-35). One of ordinary skill in the art at the time of the applicant's invention would have modified the combination of leki-Chen-Bosen so that an attribute is read before data on the card is edited. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the leki-Chen-Bosen because it would have heightened security. Reading an attribute before processing a command or program allows the combination to inhibit editing depending on the attribute. Furthermore,

using the attributes inhibits the execution of a command. Therefore, unwanted commands or programs will not start if the attribute is set to a certain value.

15. As per claim 11, leki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). leki-Chen-Bosen does not teach the transmission attribute inhibiting editing. Drupsteen further discloses the use of attributes to inhibit or allow certain commands to be processed (col 5 ln 1735). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the lekiChen-Bosen combination because it would have heightened security. Using attributes allows the system to inhibit the execution of a command. Therefore, unwanted commands or programs will not start if the attribute is set to a certain value.

16. As per claim 12, leki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). leki further discloses data copied into the memory in delayed time (see for example; fig 1 and cot 4 ln 63-67; the data being written into the card is enciphered first by a host, thus creating a delay before it is copied).

17. As per claim 13, leki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 1). Chen further discloses the card being a multi-application card (see for example; col 3 ln 41-51). leki-Chen-Bosen does not explicitly teach data being associated with respective management codes. Drupsteen discloses respective management codes for each application (K3*, col 5 ln 1-16). Chip cards contain processors, which can be programmed for different tasks. One of ordinary skill in the art at the time of the applicant's invention would have modified the combination of leki-Chen-Bosen so as to incorporate different

management codes for each application. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the respective management codes of Drupsteen within the Ieki-Chen-Bosen combination because it would have heightened security. The use of respective management codes will insure that one the data pertaining to certain applications are processed.

Response to Arguments

18. Applicant's arguments filed on September 16, 2004 have been fully considered but they are not persuasive. With respect to claim 1, applicant argues that the cited portions of Ieki (US Patent 5,204,512), Chen (US Patent 5,694,471) and Bosen (US Patent 5,060,263) do not teach the process where the second card stores data relating to the first card as recited in claim 1. The examiner respectfully disagrees.

The examiner would point out that Ieki teaches data relating to the first card and second management code are recorded in a second memory of a second chip of the second chip card (i.e., IC2 stores code number or password, IC1 & IC2 further stores deciphered data which is enciphered/deciphered according to stored algorithm in IC1 & IC2). The combination of Ieki, Chen and Bosen teach the claimed limitation as interpreted by the examiner. The examiner interprets the claim language in its broadest and reasonable meaning in view of the specification. Therefore, the examiner asserts that the combination of Ieki-Chen-Bosen teaches the claimed limitations as recited in the claims. Accordingly rejections for claims 1-16 are respectfully maintained.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

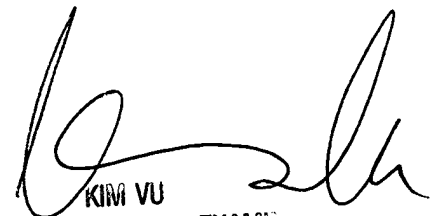
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

January 20, 2005



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135